Volume 16, Issue 08   Atari Online News, Etc.   February 21, 2014

Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1608   02/21/14

-* FCC Plans To Issue New Rules *-
-* Google To Create A Much Faster Web! *-
-* Internet A Crucial Venezuela Battleground! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""

It’s been a long week, made worse by a couple of more nasty snowstorms here in the Northeast (and elsewhere throughout the country). I have to admit, I’m spent this week! So, in essence of time - to get some rest and get this issue out, I’ll let this week go by quietly as far as some commentary goes.

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Plants vs. Zombies: Garden Warfare!
"""""""""""""""""""""""""""""

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Plants vs. Zombies: Garden Warfare Won’t Have Microtransactions

Good news for those who despise the premise of paying for things inside a game after purchasing the game, PopCap Games has announced that Plants vs. Zombies: Garden Warfare will launch without microtransactions.

This was confirmed by studio producer Brian Lindley while speaking with Gamespot.

Lindley, however, wouldn t confirm that microtransactions wouldn t be a part of the game s future. He simply stated that the studio will look at the in-game metrics and feedback from players to determine how best to move forward with the game.

In terms of the game s resolution, Lindley told Gamespot the game will run at 1080p.

On next-gen consoles, players can experience all EA games at 1080p, he said. Some are rendered natively, others are up-scaled by the next-gen hardware systems. Either way, the visuals are stunning and the gameplay is impeccable, regardless of platform.

Plants vs. Zombies: Garden Warfare launches on February 25 for Xbox One, Xbox 360 and PC. It will cost users $40 on Xbox One, and $30 for the other two platforms.

There are no plans in place to bring the game to PlayStation consoles.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

FCC Plans To Issue New ’Net Neutrality’ Rules

The Federal Communications Commission said Wednesday it will write new rules to prevent Internet service providers from charging companies such as Netflix Inc. or Google Inc. a toll to reach consumers at the highest speeds.

What does a Netflix streaming traffic jam look like from the inside? Cogent Communications CEO Dave Schaeffer discusses the heated battle between cable companies and content providers. Photo: Getty Images.

The guidelines are expected to ban broadband Internet providers from blocking or slowing down access to websites. The rule making will be the FCC’s third attempt in recent years at enforcing a concept known as "net neutrality."

Supporters say net neutrality is crucial to keeping the Internet open and allowing smaller companies to compete with the biggest content providers. But the courts have ruled against the FCC’s previous attempts to enforce net neutrality on companies like Comcast Corp. and Verizon Communications Inc. that provide Internet connections to households and businesses.

The FCC will rely on different legal arguments than in past efforts and believes it is on firmer legal footing this time around.

"The FCC must stand strongly behind its responsibility to oversee the public interest standard and ensure that the Internet remains open and fair," FCC Chairman Tom Wheeler said in a written statement. "The Internet is and must remain the greatest engine of free expression, innovation, economic growth, and opportunity the world has ever known."

Last month the U.S. Court of Appeals for the District of Columbia Circuit threw out FCC rules barring providers from blocking or slowing down websites, but acknowledged the commission has some authority to regulate broadband company practices. The FCC on Wednesday said it won’t appeal the D.C. Circuit’s ruling.

The FCC said it would likely propose new rules in the late spring or early summer, after soliciting initial public comment.

At least one Republican FCC commissioner voiced dissent. "I am deeply concerned by the announcement that the FCC will begin considering new ways to regulate the Internet," FCC Commissioner Michael O’Rielly, a Republican, said. "Instead of fostering investment and innovation through deregulation, the FCC will be devoting its resources to adopting new rules without any evidence that consumers are unable to access the content of their choice."

Any rules would have to be approved by a vote of the five-member Commission, which includes three Democrats and two Republicans.

The announcement means the FCC has thus far resisted calls from Democrats and public interest groups to reclassify broadband Internet as a public utility, which would subject the industry to much greater regulation. Net neutrality supporters argue reclassifying broadband is the only way to make the rules stand up in court, but doing so would likely provoke additional political backlash from Republicans.

Andy Schwartzman, a telecom lawyer and adviser to the anti-media consolidation group Free Press, said not doing so in the latest rule making effort "would be repeating the biggest mistake" made during prior efforts by former FCC Chairman Julius Genachowski.

Republicans on Capitol Hill remain unhappy with the FCC net neutrality effort. "The Obama administration refuses to abandon its furious pursuit of these harmful policies to put government in charge of the web," House Energy and Commerce Chairman Fred Upton (R., Mich.) and Rep. Greg Walden R., Ore.) said in a joint statement.

Sen. Edward Markey (D., Mass), said he is "pleased to see the chairman moving forward to reinstate rules on strong legal footing that preserve the open nature of the Internet."

Broadband providers have argued reclassification would be disastrous for the industry because it would subject them to regulations designed for the landline phone system.

"We think reclassification would probably be the ultimate death of the broadband market," Comcast Executive Vice President David Cohen said in an interview last week. "We think it would dry up private investment and destroy all the gains made in the broadband market in the U.S."

Mr. Wheeler has left the option open for now, which could serve as a deterrent for broadband providers seeking to challenge the rules in court again.

A Verizon spokesman said it was too early to determine whether the company would challenge any new rules crafted by the FCC. The company won’t further appeal last month’s court ruling and will continue to abide by its previous net neutrality pledge.

"Verizon remains committed to an open Internet that provides consumers with competitive choices and unblocked access to lawful websites and content," spokesman Ed McFadden said.

Comcast suggested last week it would be supportive of net neutrality rules that don’t involve reclassification. The company agreed to abide by the FCC’s net neutrality rules until 2018 to gain approval for its acquisition of NBCUniversal in 2011.

A senior FCC official said the agency expects broadband providers to uphold their commitments to net neutrality while the rule making process unfolds.

"The cable industry has always embraced the principles of an open Internet," said former FCC Chairman Michael Powell, now the CEO of the National Cable and Telecommunications Association. "We continue to believe that the values of an open Internet can be preserved, while avoiding a damaging move to heavier regulation."

As part of the process, the FCC will also examine ways to encourage competition in the broadband market. That could include removing legal restrictions that prevent cities and towns from building their own broadband or Wi-Fi networks.

Internet A Crucial Venezuela Battleground

The battle for Venezuela is being fought as vigorously online as in the streets, with authorities cutting off Internet service to a strife-torn university city and blocking selected websites and a "walkie-talkie" service widely used by protesters.

Internet connectivity was gradually restored to San Cristobal, capital of the western border state of Tachira, on Friday morning after an outage of more than 30 hours that also affected smartphones.

Soldiers patrolled the streets after another night in which police firing tear gas broke up protests just as they had the night before, when Internet service was cut. A local TV journalist, Beatriz Font, reported hearing gunshots.

"It’s an abuse!" Jeffrey Guerrero, a flour wholesaler, complained just before service was restored. "We’ve had to find out what’s happening in our city from others." He held up his iPhone to show how his Twitter service had halted.

The current wave of anti-government demonstrations, the fiercest unrest since President Hugo Chavez died last March, began in early February in San Cristobal, home to one private and three public universities.

On Thursday night, the U.S. company Zello told The Associated Press that Venezuela’s state-run telecoms company, CANTV, had just blocked access to the push-to-talk "walkie-talkie" app for smartphones and computers that has been a hugely popular organizing tool for protesters from Egypt to Ukraine.

Zello supports up to 600 users on a single channel, and company CEO Bill Moore said it became the No. 1 app in Ukraine on Thursday for both the iOS and Android operating systems. In just one day this week, Zello reported more than 150,000 downloads in Venezuela.

Venezuela’s information war escalated last week as the government blocked images on Twitter after violence in Caracas claimed three lives amid protests over woes including rampant inflation, food shortages and one of the world’s highest murder rates.

The socialist government cemented its near-monopoly on broadcast media during Chavez’s 14-year rule, and social media have been crucial for young opposition activists as they organize and exchange information on deaths, injuries and arrests.

Net-savvy activists also reported a serious nationwide degradation Thursday in Internet service provided by CANTV, which handles about 90 percent of the country’s traffic.

They said websites including NTN24.com, run by the eponymous Colombia-based regional news network, and online pastebin.com bulletin boards that cyberactivists use to anonymously share information were being blocked.

President Nicolas Maduro ordered NTN24 removed from the air last week after it broadcast video of a student killed by a gunshot to the head in Caracas.

U.S.-based company Renesys, a top analyzer of global Internet traffic, confirmed the website blocking and service degradation, but said it could not determine if CANTV was decreasing bandwidth.

"I certainly don’t know from our data if it is deliberate, although given the context, it seems plausible," said Renesys researcher Doug Madory.

Venezuela’s traffic to its close ally Cuba over the ALBA-1 undersea cable, meanwhile, appeared unaffected, he said.

Programmer and cyberactivist Jose Luis Rivas, who is from San Cristobal but did not give his location fearing persecution, said the Internet went out in most of the city of 600,000 about midnight Wednesday.

Since protests accelerated last week, activists have posted YouTube videos of riot police and National Guard breaking up demonstrations. Sometimes, the security forces are accompanied by pistol-packing motorcycle gangs of Chavista loyalists that the opposition also blames for killings and other abuses.

Rivas said that on Wednesday night, before the Internet went out in San Cristobal, people were live-streaming video of a crackdown by security forces.

Cutting the Internet deprived people of their only access to uncensored information and Rivas said people told him "they felt fear because they were no longer informed."

Government officials have not commented on the Internet outage and did not respond to Associated Press queries on either it or the service degradation and website blocking.

Spokespeople for Conatel, the government telecommunications regulator, and the Ministry of Information said they were not authorized to discuss the matter.

Conatel’s director, William Castillo, tweeted Thursday that social networks were being "invaded by cybercriminals who are attacking accounts and manipulating information."

Information Minister Delcy Rodriguez used Twitter to complain that the networks were being used to incite "coup-directed violence and create anguish."

Hacktivists also have been attacking government websites from abroad, rendering many unreachable with denial-of-service attacks, or data-packet floods.

Images, meanwhile, were visible again on Twitter after last week’s outage. Company spokesman Nu Wexler said Thursday that measures which he did not specify were taken to "ensure continuity of service." Twitter also continued to tweet a workaround that lets users in Venezuela receive tweets on their cellphones via text message.

Even before the latest round of protests, Venezuela had been blocking websites that track the black market rate for the country’s currency and for several weeks knocked out access to the popular Web address-shortening application Bitly, which was being used to get around online controls.

Venezuelans who want to reach such sites are increasingly using proxy services, which have long been employed by people in China and Iran to circumvent government censors.

The international director of the Electronic Frontier Foundation, Danny O’Brien, said he thought Venezuelan net censorship has been "somewhat haphazard and arbitrary."

Nearly half Venezuela’s population relies on government-controlled media as their sole information source, the rest on the Internet.

But cutting off Internet is not smart political strategy, said O’Brien.

"I think the important lesson people should learn from these Internet blackouts is that they just throw fuel on the flames of civil unrest."

Google Grabs Spider.io To Combat Ad Fraud

There are typically two ways to solve a technology problem: devise a solution yourself or find someone who’s working on the problem and buy their expertise.

Looks like Google has taken the second path to advance its fight against online advertising fraud; it’s bought London-based cyber security outfit Spider.io, which has made a mission out of combating click theft.

The details right now are slender, gleaned mostly by way of a post on Google’s DoubleClick Advertiser Blog that described how the short-term mission is "to include [Spider.io’s] fraud detection technology in our video and display ads products, where they will complement our existing efforts."

Based on other wording in the post, Spider.io’s tech is intended to complement other changes Google has made to its ad systems - such as, Active View, "which lets advertisers buy only those ads that are viewable on a page," and more aggressively removing bad ads from its system.

"Over the long term," the post says, "our goal is to improve the metrics that advertisers and publishers use to determine the value of digital media ... Also, by including spider.io’s fraud fighting expertise in our products, we can scale our efforts to weed out bad actors and improve the entire digital ecosystem."

The most widespread problem with ad fraud is click spoofing - using bots, or even human dupes, to generate fraudulent clicks on ads. The end result is money milked from advertisers’ pockets and into Google’s, all for ad impressions that never actually were seen - which ostensibly bothers Google a lot less than it does advertisers. But Google still has good reason to worry about ad fraud, since its entire business model depends on advertising (as ZDNet’s Ed Bott has pointed out time and again).

Google and third-party monitors of click fraud have locked horns over the extent of the problem and the question of whether Google’s or other parties’ methodologies provide more accurate measures of the problem. The fight has escalated to a legal battle more than once; in 2006, Google settled a major class-action click-fraud lawsuit to the tune of $90 million, with the terms of the settlement largely in Google’s favor.

But one of Google’s blackest eyes in online advertising came not from click fraud but from Google’s own amazingly bad judgment in selling ad space to Canadian pharmacies that were hawking prescription drugs to U.S. citizens. While Google apparently knew back in 2003 that these cross-border shipments of pharmaceuticals were illegal, it didn’t change its policies on such ad sales until 2009 - six years later, and only after it learned the Department of Justice was already on its tail. Small wonder the DOJ fined Google half a billion dollars.

The tangled web of where online ad money comes from makes it easy for even the most honest gatekeepers to be duped into funding piracy or cyber crime. (That last link leads to a discussion of the issue by none other than Douglas de Jager, CEO of Spider.io.) If Google wants to really do something about the problem of ad fraud, better technology won’t hurt, but it would be even better to follow more of where its own money comes from - if it dares.

The Next Data Theft Target: Your Medical Records

If you think Target and Neiman Marcus have done a lousy job of protecting your personal information, you may want to have a serious talk with your healthcare provider.

The impact of attacks on major retailers could be tiny compared with what s likely to happen with even more sensitive data: our electronic medical records. That s because healthcare organizations are doing an even worse job of protecting it than the big stores are, according to a report to be released tomorrow by cyber-security firm Norse Corp. and the SANS Institute, a security research and educational organization.

According to the report, millions of healthcare organizations have likely had their networks exploited by cyber-criminals or infected with malicious software that can be used to steal patients personal health information.

Norse obtained this data by setting up honeypots   sensors designed to trap malicious traffic sent across the Internet   and then it traced the data packets back to their sources. Over a 13-month period, Norse uncovered compromised machines at 375 health care organizations. Nearly three-quarters of them were doctor s offices and hospitals, with the rest divided among other healthcare-related companies.

In addition to computers and networking equipment, compromised devices included printers, video conferencing systems, call center software and X-ray machines. The danger is that attackers could use an edge system, an off-the-shelf device like a printer, to ultimately gain access to databases of patient records.

Thieves could then sell your stolen personal health information on the Internet black market, use your credentials to obtain medical services and devices for themselves and others, or bill insurance companies for phantom services in your name.

Medical ID theft is worse than financial identity theft, because there are fewer legal protections for consumers. Many victims are forced to pay out of pocket for health services obtained by the thieves, or risk losing their insurance and/or ruining their credit ratings.

According to a survey conducted by the Ponemon Institute last September, some 1.84 million Americans were victims of medical identity theft in 2013, costing them an estimated $12 billion in expenses. Two-thirds of victims said they paid nothing at all; the other third claimed to have paid an average of more than $18,000 apiece.

(Institute Chairman Larry Ponemon admits that those dollar figures are estimates and that some of the financial data collected in the survey defies easy explanation.)

Worse, someone obtaining medical services in your name could result in inaccurate information being included in your medical records   such as procedures you never had or medications you don t take   with potentially disastrous results.

Are our healthcare records at risk? Absolutely. Do healthcare providers do a poor job of protecting them? If this survey is any indication, then the answer is yes.

But it s also important to understand what the report did not say.

The report did not uncover any actual breaches of personal health information or find that attackers were targeting these organizations specifically to obtain medical records. It found no evidence that the federal insurance marketplace, HealthCare.gov, has suffered any security breaches.

The compromised systems uncovered in the survey did not include home healthcare monitoring systems or physical fitness trackers like the Jawbone UP, NikeFuel or Fitbit. While connected devices create new opportunities for hackers, there are no confirmed reports of any successful attacks on these things.

In fact, the biggest source of medical identity theft is not some hacker half a world away, it s the people in the bedroom down the hall. According to the Ponemon survey, roughly a third of all medical ID theft occurs between family members   often an aging parent without insurance who borrows a child s card. Another 30 percent is from people deliberately sharing their medical credentials with someone they know.

Only about 15 percent of medical ID theft is blamed on data breaches or deliberate attempts to steal credentials via phishing emails or fake websites, according to the survey. And that s a guess at best, Ponemon admits.

Still, the potential for cyber-theft of medical records is huge and growing larger each day. Unfortunately, as with the Target breach, there s not a whole lot consumers can do to protect their records once they re in the provider s hands. The best you can do is to keep vigilant watch over your personal health data and alert your providers if you see anything that looks wrong.

You ll want to examine the Explanation of Benefits you receive from your insurance company and request copies of your medical records from every healthcare provider, and then dispute any charges that look bogus. You ll want to keep an eye on your credit reports as well, since unpaid doctor s bills can affect your creditworthiness. And then hope that your healthcare providers learn how to do a better job of dealing with the dangers of cyberspace before they, too, get hacked.

It s not very tasty medicine, but it s what the doctor would order, if he only knew how.

How To Get Hacked in 5 Exciting Steps

Most people probably don t want to get hacked.

Most people don t want their password stolen by some anonymous Eastern European teenager. They would not like discovering that they can t get into their own email, Twitter, or Facebook accounts. They would find it embarrassing if their friends all started saying, Did you know that I m getting email spam from your account?

But come on, people. What s life without a little risk? Doesn t some danger make everything more exciting? Why do you think so many people still text and drive? Why do you think people still bike without helmets, swim right after eating, and cut off the DO NOT REMOVE tags from their mattresses?

That s right. Because risk makes everything more fun.

You ve read endless articles about how to protect yourself online. And that s fine if you re a sheep, or you re a chicken, or you want to plaster every surface of your life with bubble wrap.

But for those who seek the exhilaration of living dangerously, here it is at last: the first concise, authoritative guide to making yourself vulnerable online.

1. Choose an easy password. For years, the No. 1 most commonly chosen

password in the world was the word password.

Of course, that s also the world s most easily guessed password. And there really are professional creeps out there whose job it is to guess passwords and get into accounts. They can actually sell name/password combinations in online hacker forums.

Fortunately, we re making progress. According to SplashData s annual Worst Passwords List, password is no longer the No. 1 most used password. It s been surpassed   by 123456. Good work, people.

If you re some kind of risk-averse wussy, it s easy enough to invent a password that s not hard to memorize   but that no hacker can guess (and that no computer program can guess by trying every word in the dictionary, either). For example, you can compose a password from the initials of a fun phrase, like the delicious password 29gofiabm. (That, of course, stands for 29 grams of fat in a Big Mac.)

So, by all means, save yourself the mental strain of coming up with something hard to guess. Use password,   123456, or another one of the Top 20 like qwerty,   iloveyou, or abc123.

2. Use the same password for all your important online accounts. That s right. Use that same, easy-to-memorize password for Yahoo, Facebook, Twitter, Amazon, your bank, and your credit cards. That way, if the bad guys manage to get their hands on one of your accounts, they can also get into all your others. Now you get to live dangerously and you ve also made your life a lot easier. Only one password to memorize!

It s possible to have a different password for every site without having to be a national memory champion. You could vary the password for each website   tacking on each site s first initial at the end. For Facebook, 29gofiabmf, for example; for Yahoo, 29gofiabmy.

But you, the thrillseeker, would never bother. Nor would you bother installing a free password-management program like Dashlane or (for Apple products) iCloud Keychain. Those programs let you have a different, complex password for every site you visit   without your having to memorize anything at all!

But, hey. Where s the thrill in that?

3. Don t surrender your cellphone number as a security measure. These days, websites like Facebook, Gmail and Yahoo often ask you to provide your cellphone number.

They do that for three security reasons. First, if you forget your password or try to change it, they ll send a new one to your phone for security.

Second, if the company gets hacked or your account gets locked for security reasons, the company has a quick way to alert you   by text message   and let you know the next steps.

Third, some websites, including Google, Facebook, Twitter and Yahoo Mail, offer an optional, super-hyper-secure feature called two-factor authentication. That user-hostile term means this: The first time you log into your account from a new gadget, you have to enter a code that the company sends to you on your cellphone. In other words, hackers using their own computers can never get into your accounts unless they also have your phone.

But you know what? All that s for lily-livered pansies. Want to live on the edge? Keep your cellphone number to yourself!

4. When a bank or another company emails you to report a problem with your account, click the link and log in!

Most of the time, those are fake emails.

Clicking the link takes you to a fake website, dressed up to look like your bank s (or eBay s, or PayPal s, or Amazon s or whatever).

When you log in with your name and password, the bad guys intercept it. Now they know your name and password, so they can get into your real websites.

That particular scam   sending phony email that seems to be from your bank or another big company   is known as phishing (because they re fishing for your information, get it?). And thousands of people every year get scammed that way.

If you think that maybe there really is a problem with your bank, or eBay, or Amazon account, you could open your browser and go log into the company s website the usual way, not by clicking a link in an email.

If, however, you love the pulse-pounding adrenaline rush that comes from tempting fate, by all means   click the links in those emails and see what happens!

5. When troubles arise, pay for help. No big-name website   Yahoo, Google, Facebook, Twitter, Amazon   ever charges money to give you technical support. (Yahoo, in fact, even has a toll-free help number for I can t get into my account problems: 1-800-318-0612.)

A bunch of bogus help sites do charge you, though. They pose as tech-support agencies that can solve problems with your account   for a fee, and often if you agree to give them remote control of your computer.

Only a sucker would fall for such a scheme   or a thrill-seeker like you!

So there you have it: the five easy steps to getting hacked and scammed. Why not make life more interesting for yourself? Start right away!

You ll be in good company. Hundreds of thousands of people are already following exactly these steps today.

Google To Create Internet More Than 1,000 Times Faster

Google envisions an Internet that is 1,000 times faster than what the average U.S. user currently experiences   and it expects that vision to become a reality within three years.

 That s where the world is going. It s going to happen, Google chief financial officer Patrick Pichette said during the Goldman Sachs Technology and Internet conference on Wednesday in San Francisco, according to USA Today. Why wouldn t we make it available in three years?

That s what we re working on. There s no need to wait.

Currently, most users experience Google Fiber data transfer speeds of 1 gigabit per second, but the goal is to increase to 10 gigabits as soon as possible.

Google has had gigabit speeds in Kansas since 2012 and intends to provide similar services in Texas and Utah.

Though Google s sheer volume of user data already on file is a cause for concern to some, the plus side is that it has the money to fight draconian laws that would protect incumbent providers aiming to stymie competition, Wired magazine points out.

Nevertheless, the company s nationwide plans have already encountered obstacles. Tech website Ars Technica noted that lobbyists for corporations such as cable companies are looking for ways to stop Google through the legislative process.

Google Explores Super-Speed Internet in 9 More Cities

Google may expand its ultra-high-speed internet service into several other major metropolitan areas, including Atlanta, Phoenix, San Jose, Portland, Salt Lake City, and San Antonio.

This morning, with a blog post, the company revealed that it s considering the possibility of rolling its Google Fiber service into the regions surrounding these and four other larger American cities. The service is already up and running in Kansas City, Kansas, and it s slated to move into Austin, Texas and Provo, Utah.

When the company first revealed its Google Fiber project in 2010, it described the service   which provides internet speeds that are about 100 times faster than today s typical connections   as a mere experiment, a way of coaxing others towards faster speeds. But as Google moves to expand the service, it looks more and more like an effort to provide a very real alternative to internet connections from traditional communications giants such as Comcast, Verizon, and AT&T.

Today s news is particularly welcome because it comes on the heels of Comcast s agreement to purchase Time Warner Cable, a merger that would combine the country s two largest cable internet providers. In many ways, the Comcast deal threatens the evolution of an unfettered internet here in the U.S., but Google Fiber could provide a counter-balance, not only by improving internet speeds but by injecting some much needed competition into the market.

According to the blog post, from Google vice president of access service Milo Medin, the company is considering expansions into the greater metropolitan areas surrounding Atlanta, Georgia; Charlotte, North Carolina; Nashville, Tennessee; Phoenix, Arizona; Portland, Oregon; San Jose, California; Raleigh-Durham, North Carolina; Salt Late City, Utah; and San Antonio, Texas. In these areas, the service could eventually cover a total of 34 different cities.

But, as Google tells it, not all of these areas will necessarily receive Google Fiber. The company will work with leaders in each city to determine whether it can viably offer service to each. We aim to provide updates by the end of the year about which cities will be getting Google Fiber, Medin writes. Between now and then, we ll work closely with each city s leaders on a joint planning process that will not only map out a Google Fiber network in detail, but also assess what unique local challenges we might face. Geography, housing density, and the condition of local infrastructure will all play a role in the decision.

According to Medin, cities will also complete a checklist of items that will help them get ready for a project of this scale and speed.

The process will take a while, but Google is playing a long game. Even as it grooms the next batch of cities for its one gigabit connections, the company is also working on technology capable of boosting speeds to 10 gigabits a second   about 1,000 times faster than today s average connection. Google Fiber is no flash in the pan.

Secret Adds Subscribe/Unsubscribe Options, Post Flagging, Unlinking And More

Hot anonymous social network Secret has just pushed an update for its app that addresses a number of issues and improves performance. The new version allows users to subscribe or unsubscribe to any Secret post by swiping left, adds flagging of content that might be inappropriate, enables unlinking (more below on what that means), and speeds up the process of hearting posts.

These updates add a lot of highly requested features to Secret, which has attracted a lot of attention based on its sometimes scandalous, titillating and potentially newsmaking content. To date, however, it has offered only fairly limited functionality, with a basic stream and notifications when someone in your direct network shares something, plus updates pushed whenever someone comments or interacts with content you ve shared. The ability to subscribe means you can keep up with threads and posts you find interesting, even if you don t engage with them directly.

Flagging is another oft-mentioned feature when it comes to Secret criticism. Some have suggested that Secret might be used for bullying, and there is definitely some content I ve seen that could be potentially damaging to the reputation or livelihood of certain individuals. Secret founders David Byttow and Chrys Bader previously promised to offer more privacy controls for users, and this is a good example of exactly that kind of feature.

Another big improvement from a privacy perspective is the new Unlinking option, which allows you to remove any association between you and all of your previous posts on our servers. That means you won t be able to comment on those posts as author, get notifications, or delete them, but it also means you can t be tied to them at all.

UI improvements include the ability to swipe right to love or heart posts, and a way to not only delete your own posts, but also remove ones from others you don t want to see in your stream.

This update also helps progress Secret s efforts to foster communication between users. Subscriptions give users many more reasons to come back to the app, and to treat the network as more than just a Twitter-style stream of content that appears and disappears with a relatively short lifespan.

One complaint I ve heard about Secret from users who don t necessarily have large, Silicon Valley-based address books to draw a pool of contacts from is that the stream doesn t update frequently enough: Letting users pay closer attention to the discussions going on within posts is a good way to make even smaller networks seem more active, too.

The update should be appearing shortly for all those with the app installed.

LinkedIn Gives Users ’Member Blocking’

LinkedIn users who’d rather not receive job inquiries or other messages, or allow access to their profiles from certain other members, can now block them.

"Member blocking," was recently released by the professional social networking site after receiving requests from users. The feature adds an additional layer to privacy controls by allowing users to block profiles, direct interactions and network activity from other members with whom they do not wish to interact.

"We built this feature not only because it was a feature our members requested, but because we also knew it was the right thing to do," said Paul Rockwell, who heads trust and safety at the site, in announcing the tool.

The tool is available in a dropdown menu on the profile page, by clicking on "block or report." If a user chooses block, then the two members won’t be able to access each other’s profiles or send messages to each other. If the two are already connected, then they won’t be connected anymore if one person blocks the other.

People can view and manage their list of blocked members within a block list in their privacy and settings page.

In addition to blocking, LinkedIn also provides more granular controls to let people customize which elements of their profiles are discoverable by search engines, and who can see updates to their profile, among other settings.

With the tools, LinkedIn aims to cut down on abuse of its site and give its members a new method to prevent themselves from being spammed.

That’s if users know who they should block. LinkedIn already gives members the option to view others’ profiles anonymously. If someone enables this option, then only anonymous details about them show up, like their job title or school, when others check to see who visited their profile.

LinkedIn said that at this time, people can’t block anonymous viewers of their profile.

The Surface 2 With AT&T LTE Inches Closer To Release

Last October, Microsoft announced that it would roll out an LTE-enabled Surface 2 for AT&T s network. Sometime. The announced time frame was early 2014, and, sure enough, the device has just been found in the public FCC database, which means it s nearing release. This will be the first Surface tablet that ships with built-in cellular connectivity.

When a device hits the FCC database, it often means that it has passed the commission s battery of testing to make sure it s safe for consumers. Among other things, the FCC tests devices that transmit wirelessly. Some of these documents are released while others, often the docs that contain specific information, are held under confidentiality agreements for several weeks until the device is officially released or announced.

Around the announcement of the LTE Surface 2, there was talk of a so-called Surface Mini with a 7- to 8-inch screen hitting the market in early 2014, as well. Info on this model is still MIA. Chances are, with a device of that significance, Microsoft isn t going to let it hit the FCC database and ruin the surprise.

Facebook Turns Into A Public Memorial for Deceased Users

What happens to the Facebook profiles and accounts of users who die? The most popular social networking site has changed its policies in handling visibility of Facebook accounts of its deceased members. Thus, the Website has just allowed itself to become a public memorial for its dead users.

It should be noted that for many years now, the Website has become an instrument to memorialize profiles of dead users. Facebook locks down those members accounts.

Just recently, the Website has adjusted the restrictions on the visibility of those memorialized accounts. Thus, it is now possible for the deceased users Facebook friends to still see the profiles. Now, only Facebook friends of the dead user could see the recent public posts as well as images on the profiles of that deceased member. The site has agreed to still make those profiles visible after the death of users.

From now on, Facebook said it would keep the visibility of a dead person s content as well as account the way it had been set by that user. The recent public posts and profiles would remain public. Logically, this is making Facebook a public memorial for the dead user. It would be instrumental in keeping some memories of a deceased user alive to his family and friends who are also connected to him via the social networking site.

In a statement, Facebook said it is respecting the choices a dead user made in his life. At the same time, the Website is giving a service by allowing family and friends to still see the profile and content on the social media.

This move is now part of ways to answer several complicated questions about who should control the digital legacy of a person if he dies. Many of the bereaved are requesting access to the Facebook data and accounts of their deceased loved one. They also usually want to turn those profiles and accounts into online memorials. This may have prompted

Facebook to change some of its policies.

The Website hints that there would be more to come. It said it continues to think of more ways on how it could help users pass on and keep their memories and legacies even after their demise. Last year, Google started allowing its members to state what they prefer to happen to their profiles and data if ever they would pass away.

USPS To Commemorate Apple Founder Steve Jobs With His Own Stamp

Need to send a piece of snail mail to an Apple fanatic? Soon, there ll be a stamp for that.

The United States Postal Service will honor the late Apple co-founder Steve Jobs with his own stamp next year. According to a report from The Washington Post, which apparently acquired a secret list of future honorees, the Jobs stamp will be released in 2015 as a collectible.

Other figures who will grace U.S. postage that year include late-night host Johnny Carson, American architect Robert Robinson Taylor and as-yet-unnamed science fiction writers. The designs of these stamps have not yet been made public.

Jobs appearing on a postage stamp is somewhat ironic, of course: As the comedian BJ Novak noted on Twitter, Few people did more to crush the US Postal Service than Steve Jobs. By turning Internet-connected personal computers, smartphones and tablets into everyday devices for millions of Americans, Jobs and Apple played a large part in making email, SMS and various other messaging services (worth $19 billion or what have you) viable alternatives to what is now referred to derisively as snail mail.

Still, Jobs rose to such prominence as an entrepreneur and businessman in America that he deserved a stamp, and a stamp he will apparently get. The Steve Jobs stamp won t be here until 2015; in the meantime, if you need to find your nearest post office to pick one up   well, the USPS has a free app in iTunes that will do just that.

=~=~=~=

Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do
not necessarily reflect those of the staff, or of the publishers. All
material herein is believed to be accurate at the time of publishing.